The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. PAIGE A. THOMPSON, Defendant.	NO. CR19-159 RSL **UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS COUNTS 2 - 8**

I. INTRODUCTION

Pretrial motions under Federal Rule of Criminal Procedure 12(b) resolve legal issues that can be decided without a trial on the merits. To the extent Thompson's motion challenges the government's evidence at trial, and it should be denied for that reason alone. Further, Thompson's protestations notwithstanding, the Computer Fraud and Abuse Act (CFAA) charges against Thompson are not novel. Cases such as *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), *United States v. Phillips*, 477 F.3d 215 (5th Cir. 2007), and *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) each address situations where a person illegally accessed a computer network by "exploiting a known mistake that relates to the essential nature of [the] access." *Theofel*, 359 F.3d at 1073 (interpreting "authorization" under the Stored Communications Act to be consistent with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

"authorization" under the CFAA). Thompson's actions here constitute straightforward violations of the CFAA commonly prosecuted by the United States.

Counts 2 through 8 ("the CFAA counts") require the government to prove that Thompson intentionally accessed computers without authorization. Thompson bypassed an authentication gate, stole security credentials, and used those stolen credentials to steal data and plant malware to mine cryptocurrency. She knew that she was in a place she was not supposed to be, obtaining credentials that she had no permission to use. This is exactly the kind of external access without authorization that the CFAA prohibits.

Further, Thompson's own communications show she was aware that she was breaking the law. This severely undercuts her argument that the CFAA counts are void for vagueness as applied to her case. And the government is not infringing on Thompson's First Amendment rights to access to information or write code; rather, the government is taking the common-place step of prosecuting a computer hacker for illegal computer hacking.

II. FACTS

The facts of this case are set forth in the United States' Opposition to Defendant's Motion to Strike Cryptojacking Allegations and to Sever Count 8, incorporated herein by reference, and not repeated here. Additional facts relevant to this response are incorporated within the argument section that follows.

III. ARGUMENT AND AUTHORITIES

A. Unauthorized access includes intentionally exploiting a security flaw to gain access to private digital information.

Each CFAA count[1] requires the government to prove that Thompson accessed computers "without authorization," which is a common term in the CFAA and other technology statutes, such as the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.* Thompson claims that her access to the victim computer systems was not "without

[1] Counts 2 through 7 allege that Thompson obtained information by accessing computers without authorization, in violation of 18 U.S.C. §§ 1030(a)(2). Count 8 alleges that Thompson damaged victim computers by transmitting codes and commands to those computers without authorization, in violation of 18 U.S.C. §§ 1030(a)(5)(A).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

authorization," and therefore the CFAA counts should be dismissed as a matter of law. Aside from being a question of fact, not a question of law, Thompson is wrong about the applicable legal standard. Much like a common law trespass in physical space, courts look to accepted norms of authority and permission when analyzing intrusions in cyberspace. In this case, the Court must consider whether Thompson had permission to use certain access pathways and security credentials, and whether she used those features as they were intended to be used. Here, Thompson walked through a door that she knew had been left open by mistake, used her access to steal victim security credentials, and then used the stolen security credentials to obtain private victim data. This is unauthorized access under the CFAA.

1. Thompson lacked permission to access the victim computers and her access was unauthorized.

There are two ways to obtain information by computer in violation of section 1030(a)(2) of the CFAA: unauthorized access and exceeding authorized access. Unauthorized access means "the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission)." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009); *accord Van Buren v. United States*, 141 S. Ct. 1648, 1658 (2021). Exceeding authorized access means a person has permission to access one area of a computer system, but obtains information from another area of the system that she does not have permission to access. *LVRC Holdings LLC*, 581 F.3d at 1127; *Van Buren*, 141 S. Ct at 1658, 1662.

Thompson is an external hacker (unauthorized access), not an internal hacker (exceeds authorized access). Unlike an internal hacker, an external hacker has no authorization to access internal company systems *at all*. From the beginning, there is less ambiguity about the permissible scope of an external hacker's access to other people's computers. To the extent Thompson is attempting to characterize herself as anything other than an external hacker, that argument has no support in either the CFAA's legislative history or over 30 years' worth of cases interpreting it. *See, e.g., Brekka*, 581

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

F.3d at 1135; *Van Buren*, 141 S. Ct. at 1658; *see also Morris*, 928 F.2d 504; *Phillips*, 477 F.3d 215 (discussed in Section C, *infra*).

Thompson was not employed by any of the companies she hacked. She was not an authorized user of any of the security credentials she used to retrieve data and mine cryptocurrency. Sitting in her bedroom, she wrote a program to scan AWS clients for a specific vulnerability: an open port that allowed external internet traffic to communicate with an internal server. The port, Port 443, was supposed to block external traffic, but a misconfiguration allowed certain types of traffic to pass through to the internal server. Scanning for misconfigured ports is a bit like walking down the street, testing handles to see which doors have been left unlocked by mistake.

Once Thompson identified AWS clients with this specific misconfiguration, she wrote code to identify and assume an IAM role for each of the victim companies. An IAM role is a temporary security credential that is meant to be given by someone with authorization, to someone with authorization. The internal server gave Thompson these credentials because it mistook her for an authorized internal user. Once Thompson had the credentials, she wrote code to identify the data that was available to a person or entity who possessed those credentials. Then, depending on the permissions assigned to the credentials, Thompson copied the available data to her server and/or created new cloud servers to install and run cryptocurrency mining programs.

The entire time, Thompson knew that she was accessing private, internal computer systems because AWS clients had left Port 443 open by mistake. She knew she did not have permission to obtain or use the security credentials she obtained and used. And she did not stumble upon either the open port or the security credentials by accident; she wrote computer code to target and exploit AWS clients that had inadvertently exposed their internal servers and security credentials in this particular way.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. Authorization requires an affirmative act to grant permission, and permission is not validly obtained by manipulating and bypassing an authentication requirement.

To obscure the fact she was an external hacker who lacked internal access privileges, Thompson's motion conflates the *ability* to access information with an *authorization* to access information. Her argument presupposes that exposing private information to third parties, even inadvertently, makes that information "public," such that anyone who *can* access the information is *authorized* to access the information.[2] *See* Dkt. No. 123 at 6. The government is unaware of any case law supporting such a proposition, and the defense did not cite any.

Thompson also asserts, again without any citation to authority, that a person does not violate the CFAA by "walking through an open door." *Id.* at 7. This is an extreme oversimplification: the context of the intrusion always matters. "[D]ifferent spaces have different trespass norms." Kerr, Orin S., *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1152 (2016) ("*Norms*"). It is negligent for a person to leave the front door of his house wide open; it is still illegal for a stranger to walk into that house and steal a television. Noticing an open door is not the same as having permission to enter the house. But Thompson wants the Court to treat digital information differently. She wants the Court to proclaim new law that a security flaw transforms private digital information into "public" information everyone has a right to access. *This* is the novel legal theory, not the government's prosecution.

Thompson's theory of "inadvertent authorization" contradicts established Ninth Circuit precedent. Although the CFAA itself does not define authorization, the Ninth Circuit has ascribed that term a "clear" and "straightforward" meaning. *United States v. Nosal ("Nosal II")*, 844 F.3d 1024, 1035 (9th Cir. 2016). Authorization is an affirmative action that gives someone permission to do something. *See LVRC Holdings LLC*, 581

[2] Under Thompson's interpretation of authorized access, a person who inadvertently discloses his password to a hacker through a phishing attempt has authorized the hacker to use his password and steal his information.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

F.3d at 1133 (defining "authorization" as "permission or power granted by an authority") (quoting RANDOM HOUSE UNABRIDGED DICTIONARY 139 (2001)); *see also* BLACK'S LAW DICTIONARY (10th ed. 2014) (defining "authorization" as "[o]fficial permission to do something"). If a computer system inadvertently discloses a password or security credentials to someone who misrepresents themselves as an authorized user, that is a mistake, not authorization. *See Restatement (Second) of Torts* §§ 173-174 (explaining that consent is not a valid defense to trespass when consent is obtained by fraud, misrepresentation, or mistake).

The Ninth Circuit has applied the same affirmative interpretation of "authorization" to an analogous provision of the Stored Communications Act (SCA). *Theofel*, 359 F.3d at 1072. The SCA provides a cause of action against anyone who "*intentionally accesses without authorization* a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. §§ 2701(a)(1), 2707(a) (emphasis added). In *Theofel*, the court reasoned that federal statutes are interpreted in light of common law, and the common law analogy for unauthorized access of digital information is trespass. *Id.* at 1072; *see also* H.R. Rep. No. 99-612, at 5-6 (1986) (describing, in the legislative history of the CFAA, "the expanding group of electronic trespassers," who trespass "just as much as if they broke a window and crawled into a home while the occupants were away."); *see also Norms*, at 1146 (arguing that "concepts of authorization [under the CFAA] rest on trespass norms").

Theofel held that "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances." *Id.* at 1073. An action is not "authorized" by the victim if the intruder "procures consent by exploiting a known mistake that relates to the essential nature of his access." *Id.* The court in *Theofel* expressed concern about the very interpretation Thompson tries to advance here: "Allowing consent procured by known mistake to serve as a defense would seriously impair the statute's operation. A hacker could use someone

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

else's password to break into a mail server and then claim the server "authorized" his access." *Id.*

By assuming the IAM role—a temporary security credential that Thompson knew she obtained by a *mistake* related to a server's configuration, not by *permission*—Thompson accessed victim computers and obtained information. Under the common law of trespass, this is not valid consent to entry. *See Restatement (Second) of Torts* §§ 173-174. In addition to lacking authorization to use the IAM role, Thompson did not use that role as intended. *See Morris*, 928 F.2d at 509; *see also Norms*, at 1147, 1171-72 (proposing a rule that, "when access requires authentication, whether access is authorized should hinge on whether it falls within the scope of delegated authority the authentication implies" and asserting that "[e]xploits that circumvent authentication mechanisms" are unauthorized). Thompson trespassed in cyberspace and her access to victim computer systems was "without authorization" under the CFAA.

B. Thompson's due process rights were not violated because, in general, people understand that it is illegal to use security credentials that were not issued to them, and, as a computer programmer, Thompson herself understood this.

Due process requires a law to give "a person of ordinary intelligence fair notice of what is prohibited." *United States v. Williams*, 553 U.S. 285, 304 (2008). This is a computer hacking case, and the CFAA is the federal computer hacking statute. "Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, "[i]n intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system." *United States v. Nosal ("Nosal I")*, 676 F.3d 854, 858 (9th Cir. 2012) (quoting S. Rep. No. 99–432, at 9 (1986), 1986 U.S.C.C.A.N. 2479, 2487 (Conf. Rep.)). As discussed in the preceding section, the CFAA incorporates common law principles of trespass that are well understood by a person of ordinary intelligence. And Thompson is not a person of ordinary intelligence; she is a computer programmer who

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

worked for AWS as a systems engineer.[3] This prosecution does not violate her due process rights.

One of the CFAA's due process protections is that unauthorized access must be *intentional*. In 1986, Congress changed the *mens rea* in section 1030(a)(2) from "knowingly" to "intentionally" in order to emphasize that "intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe." S. Rep. No. 432, 99th Cong., 2 Sess., *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483. This standard focuses CFAA prosecutions on people "whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." *Id.* at 2484. There is no due process problem with that: everyone understands that intentionally intruding into someone else's computer systems and stealing information is illegal.

Thompson's motion conflates notice that an activity constitutes a crime, which is a due process question, with evidence of her criminal intent, which is a factual question. At trial, the government intends to prove that Thompson intentionally trespassed into a space where she was not supposed to be, stole victim security credentials she had no permission to use, and downloaded information she had no right to possess. Evidence that Thompson inadvertently or unintentionally trespassed might be a defense at trial, but it is not a due process problem. Thompson clearly understands that she is charged with an intentional trespass, and that either authorization or lack of intent is a defense.

Further, Thompson is wrong to claim that this prosecution is unique or novel. Prosecutions like this one have been routine since the CFAA was enacted. The seminal case in this area is *United States v. Morris*. In 1988, the early days of "the INTERNET," Robert Morris, a first-year student in Cornell University's computer science Ph.D. program infected numerous university, military, and medical computer systems with an "INTERNET worm." 928 F.2d at 505-06. To install the worm, Morris used electronic

[3] Thompson's resume advertises her proficiency in proprietary AWS technologies, including S3, EC2, and IAM.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

mail and a "finger demon" function that learned information about the vulnerabilities of the targeted computer system. Morris did not intend for his worm to damage the computers it infected, but it replicated faster than he anticipated, crashing computer systems and causing thousands of dollars in damage. *Id.* Morris was convicted of intentionally accessing computers without authorization and causing damage to those computers, in violation of a former version of 18 U.S.C. § 1030(a)(5)(A).

On appeal, Morris argued that his access was authorized because he was authorized to send electronic mail and use the "finger demon" command. *Id.* at 509. The Second Circuit disagreed, holding that "Morris's conduct here falls well within the area of unauthorized access" because he "did not use either of those features in any way related to their intended function." *Id.* Instead, "he found holes in both programs that permitted him a special and unauthorized access route into other computers." *Id.* The court noted that the whole purpose of the CFAA was to punish people "who, with access to some computers that enable them to communicate on a network linking other computers, gain access to other computers to which they lack authorization." *Id.* at 511.

Seventeen years after *Morris*, the Fifth Circuit considered *United States v. Phillips*, a case that involved scanning computer networks for security vulnerabilities and using those vulnerabilities to launch brute-force attack programs that stole encrypted data and passwords. 477 F.3d 215. Similar to Thompson, the defendant in *Phillips* used a port scan to find a "back door" into University of Texas servers. *Id.* at 218. The court expressly rejected the defendant's argument that he was an "authorized user" of these servers because he had access to the World Wide Web and had found an open door. *Id.* at 220. Instead, the court reasoned that the scope of a user's authorization is typically analyzed "on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user." *Id.* at 219. The court characterized the defendant's brute-force attack program as an improper use of the computer network designed to obtain access to digital data that he was not permitted to view or use. *Id.* at 220.

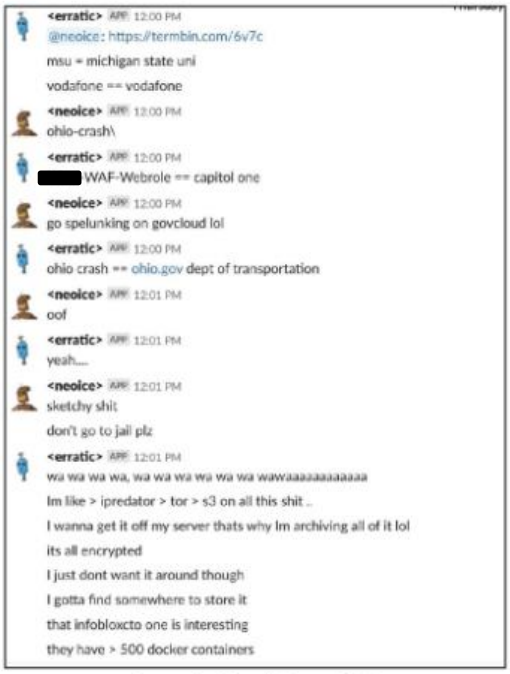
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Several years after *Phillips*, a defendant appealed his CFAA conviction in the Fourth Circuit, arguing that he was authorized to access his former employer's computer after he resigned, because his former employer forgot to change the access password. *United States v. Steele*, 595 F. App'x 208, 210 (4th Cir. 2014) (unpublished). The court rejected this argument and affirmed his conviction. *Id.* at 211.

As these cases illustrate, the *Morris* rule—that the Court should look at whether an external hacker is using programs and authentication keys as those features were intended to be used, as opposed to using those features to "find[] holes . . . that permit[] a special and unauthorized access route"—has been consistently applied in external hacking cases. *See Morris*, 928 F.2d at 505-06; *see also Norms*, at 1159-61 (advising courts to look to the *Morris* rule when analyzing the norms of trespass in cyberspace). To the best of the government's knowledge, not a single court has accepted the idea that an external hacker can gain "authorization" to a victim's computer system by intentionally finding and exploiting a flaw in a victim's defenses.

Finally, Thompson's as-applied due process challenge fails because she actually knew her activity was criminal. To begin, Thompson organized her hacking codes and stolen victim data in a computer folder named "aws_hacking_shit." And when Thompson described her activity to a fellow hacker in an online forum, the other hacker said, "sketchy shit don't go to jail plz." Thompson responded, "Im like > ipredator > s3 on all this shit . . . I wanna get it off my server that's why Im archiving all of it lol" meaning she did not expect to get caught because she was covering her tracks by using a virtual private network (iPredator) and an anonymity tool (TOR):

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



Screenshot from Netcrave Slack

Thompson knew how IAM roles work, and she knew that she was not authorized to use the IAM security credentials she stole:

> [11:43:13] <erratic> yeah aws is great, except when someone steals your IAM instance profile that has full access to the acount :)

And she made the following observation about Adrian Lamo, who was arrested, indicted, and convicted for accessing the New York Times' intranet without authorization—through a misconfigured proxy server—in violation of the CFAA[4]:

> [10:05:09] <erratic> seriously like
>
> [10:05:13] <erratic> the shit I've done
>
> [10:05:27] <erratic> way worse than what adrian lamo got arrested for initially

[4] *See United States v. Lamo*, CR04-011 (S.D.N.Y); *see also* "U.S. Charges Hacker with Illegally Accessing New York Times Computer Network," *available at*: https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/lamoCharge.htm (last visited Dec. 20, 2021); "Hacker Pleads Guilty in Manhattan Federal Court to Illegally Accessing New York Times Computer Network," *available at*: https://www.justice.gov/archive/criminal/cybercrime/press-releases/2004/lamoPlea.htm (last visited Dec. 20, 2021).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Thompson even talked about having committed "wire fraud":

> [10:06:23] <erratic> but why do I have to fuckin be the one who's trying to go to jail for wire fraud, to prove their qualified enough to have a job?

In sum, even if one could imagine a situation where a person intentionally accessed computers without authorization and stole other people's information and computing power—all without realizing she had committed a crime—that is definitely not the situation here. The Court should reject Thompson's claim that the CFAA counts violate her Fifth Amendment right to due process.

C. There is no First Amendment right to trespass in cyberspace, and, even if there were, the prohibition on external hacking does not violate the First Amendment.

There is no First Amendment right to hack other people's computers. Thompson's First Amendment claim rests on her foundational—and incorrect—proposition that, as a matter of law, private victim information was "made public" because she was able to access it. The court should reject that argument, for the reasons set forth above.

Further, Thompson's cited authorities provide no support whatsoever for the proposition that her activity was protected under the First Amendment. For example, *Sorrell v. IMS Health Inc.*, involved a law that restricted the sale, disclosure, and use of prescriber-identifying information. 564 U.S. 552, 563-64 (2011). The Supreme Court held that this was a content-based restriction on the speech of the people who lawfully held that information. *Id*. *Sorrell* has no relevance to the CFAA counts, which allege violations of a content-neutral restriction on unauthorized access to other people's computers. The CFAA criminalizes computer hacking, not speech. *See Nosal II*, 676 F.3d at 858 (focusing the CFAA on the act of computer hacking and declining to read a use-of-information restriction into that statute, consistent with the Supreme Court's later opinion in *Van Buren*, 141 S.Ct. 1648). The Supreme Court does not share Thompson's view that conduct can be characterized as "speech" simply because the person engaging in the conduct intends to express an idea. *See, e.g.*, *United States v. O'Brien*, 391 U.S. 367, 377 (1968) (rejecting a defendant's argument that a law against mutilating a draft

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

registration certificate was protected speech because the defendant burned his draft card to protest the draft and the Vietnam War).

Regardless, even if the CFAA somehow implicated Thompson's First Amendment rights, that does not mean she engaged in constitutionally protected activity. A "content-neutral regulation will be sustained under the First Amendment if it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests." *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 189 (1997) (citing *O'Brien*, 391 U.S. at 376-77). The government clearly has an important and substantial interest in protecting the privacy and integrity of digital information, which is unrelated to speech, and the prohibition on accessing other people's computers without authorization is the bare minimum necessary to further that interest. The CFAA counts do not violate Thompson's First Amendment rights.

IV. CONCLUSION

The CFAA counts are properly pleaded to provide notice of the charges against Thompson. This computer hacking prosecution is a straightforward application of the CFAA, which criminalizes intentionally trespassing into other people's computer networks. For the foregoing reasons, the Court should deny Thompson's motion to dismiss.

DATED this 23rd day of December, 2021.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

/s Andrew Friedman
/s Jessica M. Manca
ANDREW FRIEDMAN
JESSICA M. MANCA
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271